Data Encryption and Decryption using Binary-bit Sequence and Multistage Encryption

Pramod Kumar
AIIT, Amity University
Noida, India
kumarpramod017@gmail.com

Abstract: **Now days, for secured communication it is more important to use encryption process at the sender side and decryption process at the receiver side. Cryptography is a technique of shuffling the data in order to provide the security and confidentiality. It is hard to provide the security against the hacker or attacker, they can easily get the important data by finding the encryption key. Many people have developed their algorithms to provide the data security. Most of them used random key generation, and perform arithmetic operations with the key. This paper proposed a new encryption/decryption algorithm based on the ASCII, Binary-Bit sequence. In this algorithm I used logical XOR operation. This proposed method also used encryption method at the multiple stages. The key will provide by the user, will use with the XOR operation. In this proposed algorithm, the original data will be encrypted at many stages and key will also be used for encrypt the plaintext in to cipher text; same key will use to decrypt from cipher text to plain text. So this new proposed algorithm comes under the category of Symmetric key algorithms.**

Keywords: Encryption, Decryption, Plaintext, Cipher text, Key.

I. INTRODUCTION

It is the dream of every person to securely transport their message. The cryptography is the procedure by which plaintext (original) data is encrypted by a specified algorithm, the resulted text called cipher text (encrypted) data, which does not bring out the original data. The cipher text can be rearranged by a specified
Algorithm to get back the plaintext (original) data. In cryptography, the Caesar cipher is one of the oldest and more widely known encryption technique provided by the Julius Caesar. It is the substitution method in
Which each latter/word in the plaintext is replaced by the latter/word by adding or subtracting the fixed position. Caesar cipher encryption method is based on the modular arithmetic operation.
It can be represented as,
Let encrypt and decrypt the letter m by the shift of n, it can be described as mathematically as,

$$\text{Encryption, } En(m) = (m+n) \bmod 26$$

$$\text{Decryption, } Dn(m) = (m-n) \bmod 26$$

Cryptographic algorithms are classified in to two categories symmetric key and public key algorithm. Symmetric key algorithm uses the same key for encryption and decryption both process, whereas public key algorithm uses different key for encryption and decryption both process.

978-1-4673-7231-2/15/$31.00 ©2015 IEEE

Here recently developed technique named "Advance cryptography algorithm for improving data security" is discussed in [4]. In this method they describe about the encryption/decryption using symmetric key. They used initial key and key block concept in this method. Before proposing any algorithm of encryption or decryption, we have must consider about some factors like: security, features of algorithm, time and space complexity of algorithm. Fig. 1 is representing the conventional model of encryption

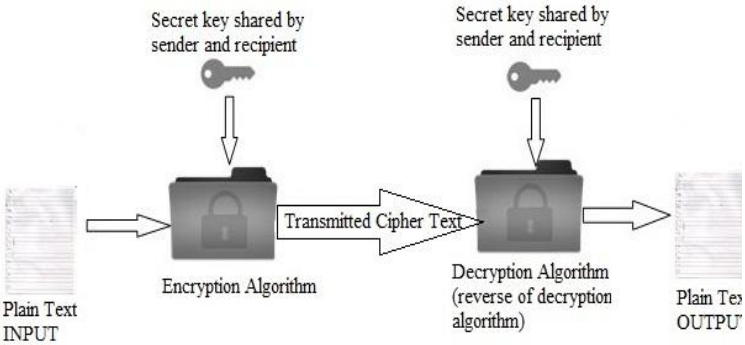

Fig. 1: A Model of Conventional Encryption

If we are looking over the security of the information then the following services are arrived: [4]

- Authentication (who created and send the data)
- Availability (performance of algorithm)
- Access Control (control use of resources)
- Confidentiality (privacy on algorithm process)

To improving the Caesar cipher by using random number generation technique for key generation technique [6]. The proposed idea suggests a method to generate the Caesar substitution key using the key matrix trace value restricted to module of 94. This method gives the enough security with high throughput and occupies minimum memory. This method is resistant against brute-force attack with 93!

Quantum cryptography, key distribution technology for the security, use of quantum cryptography in the future of information security [3]. Symmetric, Asymmetric key cryptography and random key transmission, secure way for key distribution [2]. Symmetric key cryptography using the random key generator [9]. Security of the network using the cryptography algorithm, network infrastructure, protect the network and network resources [1]. Security of the data communication, channel using the quantum cryptography [5]

Enhanced approach of the Caesar cipher algorithm and columnar transposition, but key generation should be strong [7]. Cryptographic technique at multilevel, encrypt the key used for encryption or decryption in RSA [8]. Transmit an error free image over the communication channel or the medium with efficient use of channel [10].

II. PROPOSED WORK

This paper is presenting a new symmetric cryptography algorithm. This paper is using symmetric key provided by the user. Where this key will use to encrypt the given source file or data using proposed algorithm. Basically in this technique we substitute the plain text with the cipher text by performing some operation on the binary bit sequence of the plain text. The key that will provided by the user should be from 0 to 255. Basic concept of the symmetric cryptography process is shown in Fig. 2

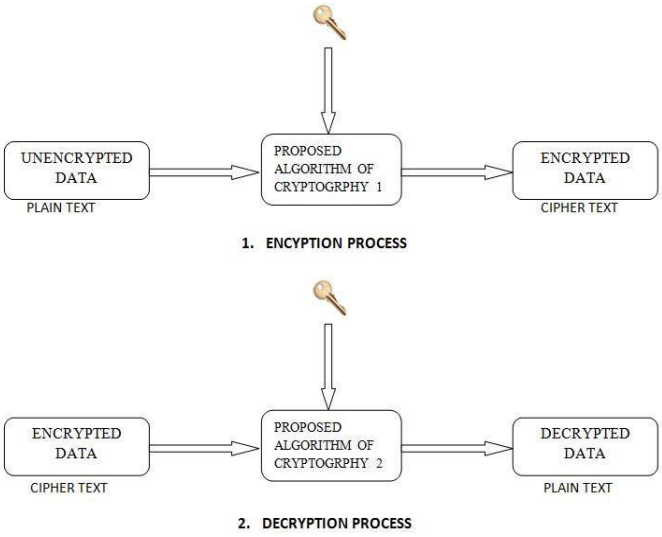

Fig. 2: Basic Concept of Symmetric Cryptography

Main reasons of using the symmetric key for encryption and decryption are:

1. Process is simple to use.
2. Security is depending on the key.
3. Sender and receiver both can use the same key and the same process for encryption and decryption.

Proposed Encryption Algorithm:

Firstly define some character values those will use to replace the plain text.

Defined characters = $2^{n/2}$

N is binary bit sequence.

1. Read the plaintext message from user.
2. Replace plaintext by their ASCII values.
3. Read a secret key from the user.
4. Perform the XOR of ASCII values with the key provide by user.
5. Convert numerical values in the binary n-bits sequence.
6. Convert the received n-bit sequence in the n/2-bits binary sequence.
7. Convert the n/2-bits binary sequence in the decimal format.
8. Change all the decimal values with respective character from the character table.
9. Transmit the cipher text.

Proposed Decryption Algorithm:

Use the same character table used in the encryption process.

1. Read the cipher text from user.
2. Replace cipher text by their numerical values.
3. Read the secret key form the user.
4. Manage the binary bits sequence.
5. Perform the XOR operation of binary bits sequence and secret key.
6. Perform reverse character substitution.
7. Process the plaintext.

III. RESULTS COMPARISONS

Here, I am comparing my proposed algorithm with RSA (Rivest-Shamir-Adleman), AES algorithm. I am comparing two parameters for execution time first one is encryption time and other one is decryption time of both algorithms. I am comparing the execution time for encrypt the plain text by the both algorithms. RSA is an asymmetric key algorithm, AES and Proposed Algorithm is symmetric key algorithm.

Here the “RSA Algorithm”, “AES Algorithm” and “Proposed Algorithm” are implemented on to the java. Compiler version jdk1.6.0_26 is used to find the execution time (in milliseconds) of RSA, AES and Proposed Algorithm. In each cycle, the same plaintexts are encrypted by copying the same plaintexts for each algorithm. I am comparing the text files only.

Finally, the outputs of execution time in the form of milliseconds in numeric form are shown in the tabular form. This is shown in table 1 and table 2.

978-1-4673-7231-2/15/$31.00 ©2015 IEEE

TABLE I
ENCRYPTION TIME COMPARISONS

Plain Text Size	RSA Algorithm	AES Algorithm	Proposed Algorithm
100 bytes.txt	45	63	2
1 kb.txt	62	64	8
2 kb.txt	78	65	24
5 kb.txt	192	112	110

TABLE II
DECRYPTION TIME COMPARISONS

Plain Text Size	RSA Algorithm	AES Algorithm	Proposed Algorithm
100 bytes.txt	141	2	2
1 kb.txt	156	2	4
2 kb.txt	169	3	7
5 kb.txt	172	8	69

Graphical representation of the table 1 and table 2 is shown in the Fig. 3 and Fig. 4 with the blue line and green line respectively for RSA algorithm and Proposed Algorithm. These observations are made using personal computer machine with the specification of Intel® Core™ 2 Duo CPU, 2.4 GHz, 2GB of RAM, Micro Soft Windows 8 (32-bit) as the testing platform.

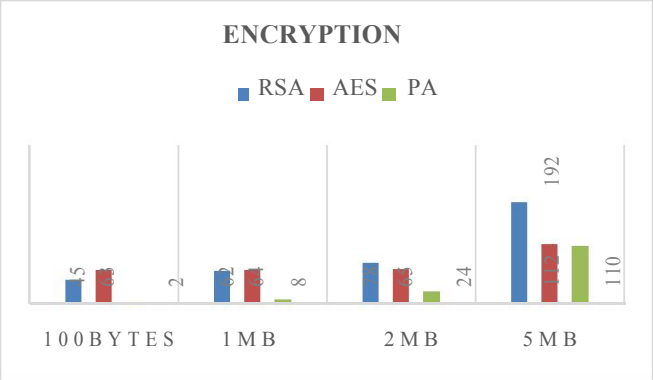

Fig. 3: Encryption Time Comparisons

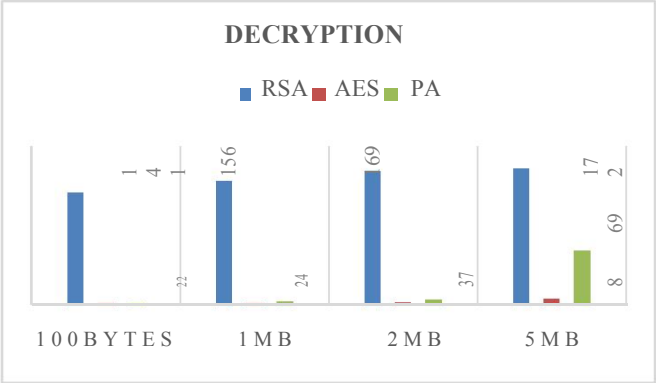

Fig. 4: Decryption Time Comparisons

IV. FEATURES OF PROPOSED ALGORITHM

Some features of this proposed algorithm are:

- Provided key for the algorithm depends on the binary bits sequence.
- Brute Force attack requires n! Attempts, so algorithm is more robust.
- Algorithm occupies minimum memory.
- Algorithm works very fast, time efficient algorithm.
- Multistage encryption is using by the algorithm.
- Algorithm is simple and more secure.

V. CONCLUSION

Data security is the most important aspect for any encryption and decryption algorithm. The space and time are also the most important aspect while designing any cipher algorithm. Our method provides high throughput by occupying less memory.

The positive thing of our proposed algorithm is that it is almost impossible to break the encryption/decryption process without knowing the exact secret key. We propose that the proposed algorithm can be applied over any type of public application to send the confidential data from one machine to another machine.

REFERENCES

[1] Ankur Singhal, Sumedha Kaushik, *"Network Security Using Cryptographic Techniques"*, IJARCSSE - 2012, ISSN: 2277 128X, V2, Issue 12, PP 105 – 107.

[2] Vidiksha, Shekher Saini, *"Data Encryption and Decryption using Deterministic Random Key for Transmission: A Review"*, IJARCSSE – 2013, ISSN: 2277 128X, V3, Issue 8, PP 817 – 818.

[3] Payal P. Kilor, Pravin.D.Soni, *"Quantum Cryptography: Realizing next generation information security"*, IJAIEM - 2014, ISSN 2319 – 4847, V3, Issue 2, PP 286 – 289

978-1-4673-7231-2/15/$31.00 ©2015 IEEE

[4] Vishwa gupta, Gajendra Singh , Ravindra Gupta, *"Advance cryptography algorithm for improving data security",* IJARCSSE – 2012, ISSN: 2277 128X, V2, Issue 1, PP 164 – 67

[5] Navleen Kaur, Amardeep Singh, Sarabpreet Singh, *"Enhancement of Network Security Techniques using Quantum Cryptography",* IJCSE – 2011, ISSN : 0975-3397,V3, No. 5, PP 1960 – 1964

[6] S. G. Srikantaswamy, H. D. Phaneendra, *"Improved Caesar Cipher With Random Number Generation Technique And Multistage Encryption",* IJCIS-2012, V2, No.4, PP 39-49

[7] Dharmendra K Gupta , Sumit K Srivastava, Vedpal Singh,*" New Concept of encryption algorithm A hybrid approach of Caesar Cipher and Columnar transposition in multi stages",* JGRCS-2012,V3, No. 1, PP 60-66

[8] K.Govinda , E. sathiyamoorth, *"Multilevel Cryptography Technique Using Graceful Codes",* JGRCS - 2011, V2, No.7, PP 1-5

[9] A.Nath, S.Ghosh, M.A.Mallik, *"Symmetric key cryptography using random key generator",* PICSAM-2010, V2, PP 239-244

[10] Ajay Sharma, Abhishek Dwivedi, Nitin Pandey, Amit Kumar, Deo Brat Ojha, *"An Approach for Two-Tier Security on Transmission of Medical Image using Post Quantum Cryptosystem over Teeming Channel"*, IJAEST-2010, V1, No. 1, PP 10 - 15

978-1-4673-7231-2/15/$31.00 ©2015 IEEE